Offre n°2025-09077

PhD Position F/M Attack Modelling of Symmetric Primitives

Type de contrat : Fixed-term contract

Niveau de diplôme exigé : Graduate degree or equivalent

Fonction : PhD Position

Contexte et atouts du poste

The main objective of the PhD project is to propose new attack modellings of symmetric primitives.
It will be carried out in the CARAMBA team at Loria, in Nancy, within the framework of the project CRYPTANALYSE of the PEPR CYBERSÉCURITÉ.

Business travels, in France or abroad, could be considered to disseminate the scientific results, in particular at conferences. Travel expenses are covered within the limits of the scale in force.

Mission confiée

Context

When designing a symmetric-key primitive, trying to attack it (a.k.a cryptanalysis) is the main approach we have to assess its security. Particular care shall be taken to the analysis of statistical attacks, which are among the most efficient approaches known to date. The
two most famous examples are differential and linear cryptanalysis, but many other variants were proposed afterwards, including the differential-linear technique and the boomerang attacks, to cite a few.

Unfortunately, no efficient ways exist to identify statistical defects, and the generic approach is to study each of the small components to deduce how the property evolves round after round through the primitive. On the bright side, several techniques have been recently introduced to automate this process with computer programs, saving cryptanalysts from having to do it manually. It however remains imperfect as the descriptions of the problem in the programs (known as the modelling techniques) are generally simplifications that are not always accurate, and are often unsuitable for lightweight constructions.

PhD proposal

In recent years many new iterative frameworks that aim at capturing more accurately the probability have been proposed. While their theory is in general sound, they are harder to use, and it is less clear how to efficiently find distinguishers with these approaches.
The aim of this PhD is to propose new modelling techniques for automated search of symmetric distinguishers and attacks.

Principales activités

The core activities of this PhD thesis include:

- Study the state-of-the-art in the modelling of attacks and the recents theoretical frameworks giving estimates of the probability of distinguishers,
- Develop new methods for modelling the search of efficient parameters for a cryptanalysis,
- Write and publish the scientific results in scientific journals and conferences.

Compétences

- Solid knowledge in the domain of cryptography.
- Solid programming skills (Python, Sagemath, C).
- Strong communication abilities.
- Fluency in English (written and spoken)

Avantages

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours
- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

Rémunération

2200€ gross/month

Informations générales

- **Thème/Domaine :** Algorithmics, Computer Algebra and Cryptology
- **Ville :** Villers lès Nancy

- **Centre Inria :** Centre Inria de l'Université de Lorraine
- **Date de prise de fonction souhaitée :** 2025-10-01
- **Durée de contrat :** 3 years
- **Date limite pour postuler :** 2025-08-02

Contacts

- **Équipe Inria :** CARAMBA
- **Directeur de thèse :**
  Bonnetain Xavier / xavier.bonnetain@inria.fr

A propos d'Inria

Inria est l'institut national de recherche dédié aux sciences et technologies du numérique. Il emploie 2600 personnes. Ses 215 équipes-projets agiles, en général communes avec des partenaires académiques, impliquent plus de 3900 scientifiques pour relever les défis du numérique, souvent à l'interface d'autres disciplines. L'institut fait appel à de nombreux talents dans plus d'une quarantaine de métiers différents. 900 personnels d'appui à la recherche et à l'innovation contribuent à faire émerger et grandir des projets scientifiques ou entrepreneuriaux qui impactent le monde. Inria travaille avec de nombreuses entreprises et a accompagné la création de plus de 200 start-up. L'institut s'e?orce ainsi de répondre aux enjeux de la transformation numérique de la science, de la société et de l'économie.

Attention: Les candidatures doivent être déposées en ligne sur le site Inria. Le traitement des candidatures adressées par d'autres canaux n'est pas garanti.

Consignes pour postuler

Sécurité défense :
Ce poste est susceptible d'être affecté dans une zone à régime restrictif (ZRR), telle que définie dans le décret n°2011-1425 relatif à la protection du potentiel scientifique et technique de la nation (PPST). L'autorisation d'accès à une zone est délivrée par le chef d'établissement, après avis ministériel favorable, tel que défini dans l'arrêté du 03 juillet 2012, relatif à la PPST. Un avis ministériel défavorable pour un poste affecté dans une ZRR aurait pour conséquence l'annulation du recrutement.

Politique de recrutement :
Dans le cadre de sa politique diversité, tous les postes Inria sont accessibles aux personnes en situation de handicap.